

REMARKS

Claims 1-10 are currently pending with claims 1 and 7 being independent. Claims 11 and 12 have been newly added. Favorable reconsideration of the action mailed on November 25, 2009 is respectfully requested in view of the following comments of the Applicant, which are proceeded by related comments of the Examiner in small bold type.

Examiner Interview

Applicant's representatives Mr. Jeffrey J. Barclay (Reg. No. 48,950) and Mr. Jeffrey D. Weber (Reg. No. 64,828) would like to thank the Examiner for the telephone interview attended February 2, 2010. In accordance with MPEP Section 713.04, the substance of the interview is included herein.

Along with the independent claim 1, the specification of the subject application was discussed along with the rejections from the subject action. Potential claim amendments were also discussed.

Claim Rejections

Claims 1-10 are rejected under 35 U.S.C. 102(e) as being anticipated by Challenger et al. (D. S. Patent 6,718,468).

Nothing in Challenger discloses or renders obvious at least "generating a first key from a user-supplied unencrypted password" and "encrypting the user-supplied unencrypted password using the first key" as recited by amended claim 1.

Instead, Challenger discloses two instances of data encryption. First, a public key (referred to as a chip public key) is used to encrypt a random password and a public/private key pair. In this regard, Challenger states:

Starting at block 40, a user public/private key pair is first received by a signature chip (such as signature chip 31 from FIG. 1), as shown in block 41. Typically, this user public/private key pair has already been certified with the

proper authority. A random password, preferably 64 bits in length, to be associated with the user public/private key pair is then generated for the user, as depicted in block 42. This random password, which is preferably generated by a random generator, is typically very difficult for a human user to remember. Utilizing a chip public key, the random password is then encrypted along with the user public/private key pair, as shown in block 43. (Challener, col. 4 lines 11-22)

Second, the chip public key is used to encrypt a first password generated from a hash phrase and the random password. In this regard Challener states:

Next, a first password is generated by hashing a first pass phrase, as shown in block 45. A pass phrase is utilized because a pass phrase permits greater permutation, and thus added security, not to mention a pass phrase is easier for a human user to remember than the random password. Utilizing the chip public key, the first password is then encrypted along with the random password, as depicted in block 46. (Challener, col. 4, lines 30-37).

As such, for both instances described by Challener, a chip public key is used to encrypt corresponding data. Not being generated from a user-supplied unencrypted password, Challener's chip public key is not equivalent to the first key of amended independent claim 1.

Further, as described in the reply filed 6 July 2009 in response to the office action of 5 February 2009, Challener's public key used for encrypting is completely unrelated to the information being encrypted. Challener's pre-existing key is provided from chip storage (see column 4, lines 22-23) and has no knowledge of or relationship whatsoever with user supplied information. As such, the reference does not describe or suggest generating a first key from a user-supplied unencrypted password, and encrypting the user's password with the first key, as required by claim 1.

Amended independent claim 7 and newly added independent claim 11 contain similar subject matter amended independent claim 1 and are allowable for at least similar reasons.

Dependent claims 2-7, 8-10 and 12 properly dependent on independent claims 1,7 and 11 and respectively and are allowable therewith.

It is believed that all of the pending claims have been addressed. However, the absence of a reply to a specific rejection, issue or comment does not signify agreement with or concession of that rejection, issue or comment. In addition, because the arguments made above may not be exhaustive, there may be reasons for patentability of any or all pending claims (or

other claims) that have not been expressed. Finally, nothing in this paper should be construed as an intent to concede any issue with regard to any claim, except as specifically stated in this paper, and the amendment of any claim does not necessarily signify concession of unpatentability of the claim prior to its amendment.


In view of the foregoing amendments and remarks, Applicants respectfully submit that the application is in condition for allowance, and such action is respectfully requested at the Examiner's earliest convenience.

Applicants' undersigned attorney can be reached at the address shown below. All telephone calls should be directed to the undersigned at (617) 368-2191.

The fee of \$245 for the Petition for Extension of Time is being paid concurrently herewith on the Electronic Filing System (EFS) by way of Deposit Account Authorization. Please apply any charges or credits to deposit account 06-1050, referencing Attorney Docket No. 13984-0005US1.

Respectfully submitted,

Date: 26 April 2010



Jeffrey J. Barclay
Reg. No. 48,950

Fish & Richardson P.C.
Telephone: (617) 542-5070
Facsimile: (877) 769-7945